安天发布《Montserrat 勒索软件分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Montserrat 的勒索软件，Montserrat 勒索软件于 2019 年 12 月初被发现，主要通过钓鱼邮件进行传播，邮件附件中包含一个名为 Windows backup storage.exe（Windows 备份存储）的勒索程序，目的是伪装成 Windows 系统中的备份功能程序，诱使用户运行该勒索程序。

Montserrat 勒索软件执行后，加密计算机上的文件，在原文件名后追加名为“.encrypted_backup”的后缀，将 %User% 目录下部分文件（例如图片、音乐和视频等）的中文名修改为相同意义的英文名（例如图片目录下的“沙漠 .jpg”修改为“Desert.jpg.encrypted_backup”），在所有含有被加密文件的位置创建名为“How to restore data.html”的勒索信，勒索信内容包含勒索说明、联系邮箱和 USER_ID 等。Montserrat 勒索软件使用“RSA+AES”加密算法加密文件，调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本、禁用修复、删除本地计算机的备份目录等。目前被加密的文件在未得到密钥前暂时无法解密。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免一切勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的口令；确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。

目前，安天追影产品已经实现了对该类勒索病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、字符串分析鉴定器、关联分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据关联分析鉴定器、关联分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	4113f6779e90492afa8c61886998189194a42cb3438517b205c8fa10e5862051
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	825 KB
MD5	EF7CD02F86BCA22547ECF4E6B10F2A9F
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Exploit]/Win32.Generic
判定依据	动态行为

◆ 操作系统

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
查询系统硬盘大小	★★★
堆喷射	★★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
获取计算机名	★
镜像劫持	★★
检索系统内存信息	★
获取系统版本	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
枚举服务	★
.....	.....

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 12 月 16 日 (总第 212 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天入选工业和信息化部网络安全威胁信息共享平台合作单位

12 月 9 日，以“共建网络安全生态 保障网络强国建设”为主题的 2019 年中国网络安全产业高峰论坛在北京召开。本届论坛由工业和信息化部、北京市政府共同指导，工业和信息化部网络安全产业发展中心、北京市经济和信息化局、北京市通信管理局、海淀区政府联合主办。工业和信息化部副部长陈肇雄、北京市副市长殷勇出席论坛开幕式并致辞。

论坛上发布了国家工业互联网安全态势感知与风险预警、工信部网络安全威胁信息共享两大平台，并为网络安全试点示范项目和网络安全威胁信息共享平台合作单位举行授牌仪式。

安天凭借自身在网络安全领域的核心技术实力和专业的安全服务能力入选首批“工业和信息化部网络安全威胁信息共享平台合作单位”。

同时，安天申报的黑龙江省网信办态势感知与监测预警平台以及与中国民航大学共同申报的民航网络与信息安全管理平台两个项目入选工信部网络安全技术应用试点示范项目。

安天监测型态势感知平台，由网站监测、重要信息系统监测、甄别研判、通报预警、协调指挥、应急处置、态势可视化以及系列探针和工具等组件组成。主要面向安全监管部门、行业主管部门及集团企业等安全监测、监管场景，可实现威胁与隐患统一发现、网络安全态势综合评估、安全决策辅助制定、多方资源协调联动，进而实时、高效、切实保障关键信息基础设施安全，加强履行监管部门的网络安全监管的职责，助力打造牢固的网络安全防线。

安天承建了民航网络与信息安全管理平台，多方面保障民航安全，及时提供应急服务支撑。在中国 C919 大飞机首飞、中国商飞、北京市交通委网络安全管理体系建设等重大项目中安天承担了重要角色，并获得了客户的一致好评。

未来安天将加大研发投入，促进技术创新发展，不断优化提升项目的实用性和可推广性，有力支撑试点示范项目在网络安全领域的应用推广。

微信扫描二维码阅读原文

勒索软件 Zeppelin 通过供应链攻击传播

据研究人员称，Zeppelin 通过受管理的安全服务提供商 (MSSPs) 在供应链攻击中传播，这种攻击方法类似于 Sodinokibi 勒索软件。该恶意软件具有很高的可配置性，可以作为 EXE，DLL 文件或捆绑到 PowerShell 加载程序中进行部署，但是无论以哪种方式提供，Zeppelin 都使用一个名为 .zeppelin 的临时文件夹开始安装，然后在目标机器上传播。当勒索软件侵入网络时，它会使用私钥加密文件，将受害者与其他攻击目标区分开，攻击者甚至可以通过监视 IP 地址来确保锁定目标。文件全部加密后，Zeppelin 将在文本文件中向受害者提供赎金记录。

（原文链接：https://www.zdnet.com/article/this-new-ransomware-is-targeting-health-and-tech-companies-across-europe-and-north-america/）

Adobe 发布了其 2019 年 12 月安全更新补丁

Adobe Systems 修复了 Acrobat Reader，Photoshop 和 Brackets 中的 17 个漏洞，如果被利用，则可能导致任意代码执行。总体而言，作为定期更新的一部分，Adobe 发布了补丁程序，解决了包括 Acrobat Reader PDF 查看器在内的各种产品中的 25 个 CVE。Adobe 表示，到目前为止，尚未流行针对这些漏洞的攻击。

（原文链接：https://threatpost.com/adobe-fixes-critical-acrobat-photoshop-brackets-flaws/150970/）

土耳其银行数据泄露暴露约 46 万条用户记录

Group-IB 是一家总部位于新加坡的网络安全公司，该公司在最受欢迎的地下卡店之一中检测到大量的借记卡和信用卡记录，其中大部分与土耳其最大的银行有关。在 10 月 28 日至 11 月 27 日之间，总共上传了 460,000 条记录。发现此数据库后，Group-IB 将有关付款记录的出售通知了适当的地方当局。

（原文链接：https://techcrunch.com/2019/12/09/birth-certificate-applications-exposed/）

每周安全事件

类 型	内 容
中文标题	埃塞俄比亚因网络攻击暂时关闭了互联网
英文标题	Ethiopia briefly shut internet as a cyber attack hits
作者及单位	borkena
内容概述	埃塞俄比亚信息网络安全局（INSA）周四表示，针对该国金融机构的网络攻击已经被阻止。在此过程中，该机构表示，根据国家隶属的 Fana Broadcasting Corporation（FBC）的报道，该机构被迫关闭该国家长达 20 分钟的互联网。没有具体说明哪些金融机构是网络攻击的目标。
链接地址	https://borkena.com/2019/12/05/ethiopia-briefly-shut-internet-as-a-cyber-attack-hits/

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别	名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.Locker.bz[rog,lck] 2019-12-08	高	该应用程序被恶意篡改，植入了恶意代码，运行会锁定用户界面，要求用户付费解锁，影响用户手机的正常使用，请立即卸载。
		RiskWare/Android.IappShare.o[exp,rog] 2019-12-09	低	该应用程序运行诱导用户加入 qq 群，进行分享推广引流。警惕应用包含色情内容，可能造成用户资费消耗，存在一定的风险，建议谨慎使用。
		RiskWare/Android.IappShare.q[exp] 2019-12-10	低	该应用程序用裕语言编写，伪装色情应用或辅助工具，运行诱导用户分享软件，加入 qq 群，存在被诱骗欺诈的风险，请卸载。
	较为活跃样本	RiskWare/Android.Fakejiaoyou.j[fra,exp]	中	该应用程序伪装交友软件，通过发送虚假诱惑性消息，以及特权服务，诱导用户付费，造成用户资费损失，建议卸载。
		Trojan/Android.SmsSpy.cn[prv,exp]	中	该应用程序运行监听用户短信并发送到指定号码，造成用户隐私泄露和资费损耗，建议卸载。
		RiskWare/Android.Dropper.dt[exp]	低	该应用程序包含风险代码，运行后频繁推送广告，可能会加载子包，造成用户资费损耗，请谨慎使用。
		G-Ware/Android.HiddenAds.jx[exp,rog]	低	该应用程序安装无图标，运行加载子包，后台推送广告，造成用户的资费消耗，建议不要使用。
		RiskWare/Android.FakeQQ.av[fra]	低	该应用程序伪装成 qq，非官方应用，无实际功能，建议使用官方正版应用。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Jet 数据库引擎远程代码执行漏洞（CVE-2019-1406）	高	当 Windows Jet 数据库引擎不正确地处理内存中的对象时，存在远程执行代码漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码，攻击者可以通过诱使受害者打开经特殊设计的文件来利用此漏洞。
	较为活跃样本	Trojan[FakeAV]/Win32.Onescan	中	此威胁是一种通过将自身伪装为安全软件的方法来传播的木马类程序，以发现虚假威胁诱使用户在线充值为目的。该家族伪装成反病毒软件的木马程序。该家族会弹出虚假报警恐吓用户，提示用户如果想彻底查杀家族必须购买软件，并提示用户使用信用卡支付。该家族使用扰乱用户正常使用电脑的策略，骗取用户对软件付费。
		Trojan[Exploit]/Win32.Serv-U	中	此威胁是一个基于 serv-u 软件的有后门行为的木马家族。该家族的样本在执行后，攻击者即获得对此设备的完全控制权限。
		Trojan[Backdoor]/Win32.KillDientes	中	此威胁是一个具有后门行为的木马家族。该家族的样本在执行后，攻击者即获得对此设备的完全控制权限。
		Trojan[Backdoor]/Win32.Vawtrak	中	此威胁是一种带有后门的木马类程序。该家族会在后台访问恶意网址。该家族运行后注入到所有进程中，可以链接到 IRC 服务器获取恶意指令。
		Trojan[Ransom]/Win32.Kerlofost	中	此威胁是一种具有勒索行为的木马类程序。它可以加密用户数据并要求用户付费解密，否则数据就会被破坏，有一定威胁。

2020 年五大网络安全预测

Liron Barak/ 文 安天技术公益翻译组 / 译

要想保护网络安全，重要的是要领先于威胁一步，而非被动地对威胁做出响应。在不断变化的威胁形势下，仅仅填补漏洞——或针对昨天的威胁设计安全措施，已经远远不够了。新的一年即将到来，新的威胁和趋势也会随之而来，特别是在网络安全领域。接下来，我们将汇总 2020 年五大网络安全预测，以帮助企业防范威胁。

勒索软件威胁将更加严重

• 勒索软件越来越复杂。

• 甚至能够规避最先进的电子邮件安全解决方案。

• 会导致更具破坏性的后果。

现在，勒索软件攻击能够以更高的复杂度和自动化程度（尤其是在创建木马变种方面），规避最先进的电子邮件安全解决方案。更重要的是，当前的安全解决方案在勒索软件攻击发生几小时后才开始检测，而这时破坏已经造成了。

我们以银行木马 Emotet 为例进行说明。Emotet 大获成功的原因之一是它利用了特定目标，因此声誉服务需要更多的时间来检测它。此外，Emotet 不断改变“攻击信标”（IOC），因此即使是最新的特征、IDS 和其他传统解决方案也无法快速检测到它。

正如我们所见，这些攻击大约每隔一周就会发生一次。攻击者开发了一个新的样本库，并在样本中嵌入新的模糊和规避技术。然后，他们对这些样本进行排列组合然后传播。在攻击者为样本创建新的技术时，安全厂商必须迎头赶上。

与网络钓鱼攻击相关的风险将是安全主管最关注的问题

• 我们一直听说，各方面的安全专家正在寻找解决方案来解决日益增长的网络钓鱼攻击风险。

• 一年前，恶意软件被认为是企业面临的最大威胁。随着我们迈入 2020 年，网络钓鱼攻击将成为主要威胁。

如今，大多数希望增强其电子邮件安全性的企业，都需要阻止网络钓鱼攻击。网络钓鱼攻击越来越复杂，即使是最专业的安全人员也无法检测到所有攻击。暗网上提供的网络钓鱼工具包以及面向针对性攻击的被盗凭证列表，意味着网络钓鱼攻击的数量和复杂程度也将增加。

此外，网络钓鱼攻击的后果会更加严重。数据泄露、金融诈骗，以及网络钓鱼攻击的其他后果，可能会对各种规模的企业带来灾难。根据 Verizon 公司《2019 年数据泄露调查报告》，网络钓鱼是造成数据泄露的首要原因。

企业需要能够检测和阻止此类攻击（尤其是通过电子邮件传播的攻击）的技术。

迅速发现威胁的需求将更加紧迫

• 一旦威胁入侵，就会开始对企业造成破坏。

• 数据驱动的安全解决方案需要花费数小时才能检测到未知威胁。

• 这是攻击的最危险阶段。

• 企业对这种反应时间的容忍度将越来越低。

攻击对受害者造成最大破坏性影响的时间范围是：从恶意载荷被释放到安全解决方案检测到恶意载荷。即使是最先进的安全解决方案，通常也要花费几个小时（甚至更长的时间）才能检测到新的未知攻击，因此这个时间窗口内的风险很大。

企业和安全专家已经开始意识到这一点，预计会将其视为 2020 年的一个关键挑战。

企业协同平台将成为更受攻击者青睐的攻击向量

• 更多的攻击者将利用云盘和即时通讯程序等平台。

• 这些企业协同平台通常会立刻受到用户的信任——而攻击者将会利用这一点。

协同服务的使用呈爆炸式增长。越来越多的用户开始使用微软 OneDrive，Google Drive 等工具进行协同。虽然这对于提高生产率非常重要，但是对安全专家带来了独特的挑战。

这些服务不断遭受攻击——攻击频率、复杂性和规避手法不断提高。新的服务带来了新的攻击向量，这也意味着风险和潜在损害也会不断增加。

数据泄露和攻击模拟（BAS）供应商会将其解决方案扩展到各种渠道和攻击向量

• Gartner 指出，大多数威胁仍然通过电子邮件传播。

• 在检测到的恶意软件中，通过电子邮件传播的占 94%。这类攻击在 2018 年造成了超过 12 亿美元的损失。

• BAS 工具通过模拟网络攻击来测试网络的防御能力，但面向电子邮件的 BAS 尚未成为主流。

预计 BAS 供应商会将其解决方案扩展到整个杀伤链，从而为客户提供更全面的解决方案。电子邮件是一种热门攻击向量，因此 BAS 供应商的解决方案很可能也会开始覆盖电子邮件。

2020 年网络安全预测：未来的挑战

包括电子邮件在内的工具提高了工作速度、效率和协作，也为安全团队带来了更多的风险和漏洞。无论攻击者利用勒索软件、网络钓鱼还是热门协同平台，我们的目标始终是保护用户和企业的安全。

在我们提供安全产品来防御威胁的同时，攻击者也在不断创新以规避安全技术。

很明显，企业不能依靠 2019 年的解决方案来保护新一年的安全。在这种情况下，网络安全专家的作用显得更加重要。我们将迎来激动人心的一年，新的威胁、新的挑战以及一个日益互联的世界也会随之而来。在这新的一年里，企业需要安全专家的帮助来确保安全性。

原文名称	Top 5 cybersecurity predictions for 2020
作者简介	Liron Barak。Liron Barak 是 BitDam 公司首席执行官。
原文信息	2019 年 12 月 9 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2019/12/09/cybersecurity-predictions-2020/
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。